Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1317 04/29/10

~ Web Security Questions ~ People Are Talking! ~ Net Survives Royals!
~ MS: Go and Sin No More ~ PlayStation Net Outage ~ PSN Outage Update!
~ Wii Successor in 2012! ~ Sony Shows S1 Tablets! ~ FBA Probes Troubles!

~ Computer Mouse Hits 30 ~ Twitter Blast Hits Sox ~ New Firefox 4 Add-Ons!

-* Amazon Apologizes for Outage *-
-* ICANN Names Hacker As Security Chief *-
-* NY Case Underscores Wi-Fi Privacy Dangers! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, nothing that I could say tonight could come close to being as entertaining as what occurred earlier today, the Royal Wedding of Prince William and Kate Middleton. Now, I'm not usually a person who pays a whole lot of attention to the British monarchy, but I do have to admit that they do pique my interest from time to time.

Whether we like it or not, most of us have grown up with the British royalty, especially Charles and Diana some 30 years ago. It's hard to ignore the growing up of their sons, up to this joyous event.

So, while the partying continues into the wee hours of the night and next morning in England, we still have to take care of business here!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Wii Successor Coming in 2012!
"""""""""""""""""""""""""""""""" PlayStation Network Outage!
PS Network Update!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Nintendo Says Successor to Wii Coming in 2012

The successor to Nintendo's hit Wii console will arrive next year.

In disclosing its plans Monday, Nintendo Co. didn't say what the new

system will do. The Japanese company plans to show a playable model of the new console at the Electronic Entertainment Expo, which runs June 7-9 in Los Angeles.

Nintendo has dominated sales of video game consoles and sold 86 million Wiis since launching it in 2006. The Wii caused a splash with its innovative motion-sensing controller. Sports-style games such as baseball and boxing let players move their arms to simulate the pitching of a ball or the throwing of a punch. Nintendo also makes a step-board accessory, the Wii Fit, that allows players to try dance steps or yoga.

The Wii setup has been copied and elaborated on by the other major console makers since then.

But the Wii is showing its age. Even when it launched, it was behind the other consoles of the era, Sony Corp.’s PlayStation 3 and Microsoft Corp.’s Xbox 360, in not offering a high-definition image.

The modest hardware of the Wii has also meant that while Sony and Microsoft have been able to update their consoles with new capabilities, the Wii has seen only relatively minor updates, such as addition of the optional Wii Fit and the ability to play Netflix movies.

Microsoft launched its Kinect game-control system last fall. Using a 3-D camera, depth sensors and voice-recognition software, it recognizes your face, voice and gestures as you move around and talk, without requiring you to hold a controller or wear a headset. Sony, meanwhile, began selling a Move controller that is essentially a higher-tech version of the Wii remote.

Nintendo announced plans for the Wii successor as part of its financial results Monday. Nintendo said its annual earnings dropped for the second straight year as sales declined. It’s expecting sales to increase again in the fiscal year that just started, thanks to its new handheld 3DS device, which launched last month.

PlayStation Network Outage Blamed on ’External Intrusion’

Sony’s PlayStation Network and its Qriocity music service were still down Monday afternoon, with no word on when they will be back online. On Friday, the company reported that the downtime was caused by "an external intrusion" to both services.

Patrick Seybold, senior director of corporate communications and social media, posted on the company’s PlayStation Blog on Friday that, "in order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward," both PlayStation Network and Qriocity were turned last Wednesday. Sony has noted that it doesn’t know the degree to which personal data might have been compromised.

On Monday, Seybold posted that he knows users are "waiting for additional information on when PlayStation Network and Qriocity services will be online." He added that, "unfortunately, I don’t have an update or time frame."

With several major new game titles coming out this week, the timing of

the outage is particularly suspicious. Many observers have speculated that the "external intrusion" was caused by the Anonymous hacker group.

But Anonymous denies involvement, while simultaneously posting updates to its Facebook page that suggest it could have been involved. On its AnonNews web site, where anyone can post, there is a notice dated Friday titled For Once We Didn't Do It. The posting noted that, while some individual Anons could "have acted by themselves," AnonOps was not involved and "does not take responsibility for whatever has happened."

The posting added that the "more likely explanation is that Sony is taking advantage of Anonymous' previous ill will toward the company to distract users from the fact that the outage is actually an internal problem with the company's servers."

However, on Anonymous' Facebook page, the page owner posted in a discussion of the outage last week that "we have no qualms about our actions."

In early April, several Sony sites were brought down by members of Anonymous, the hacker group known for its politically oriented online attacks. The sites included Sony.com, Style.com and the U.S. site for PlayStation.

Before the attacks on the Sony sites, Anonymous had announced it would target the company because of Sony's lawsuit against a user named George Hotz. Sony had filed and received a restraining order against Hotz and other hackers for allegedly jailbreaking the PlayStation 3 game console in order to run unauthorized software such as pirated games, and for providing software tools for others to do the same.

Sony had also sought and received access to Hotz' social-media accounts, and the IP addresses of visitors to his web site. The company also obtained access to his PayPal account to see donations in support of his jailbreaking efforts.

In an open letter to Sony, Anonymous said Sony "abused the judicial system in an attempt to censor information on how your products work." It added that the company "victimized your own customers merely for possessing and sharing information," and said these actions meant Sony had "violated the privacy of thousands."

Sony and Hotz reached a settlement several weeks ago. The terms of the agreement were not made public, although Hotz agreed to a permanent injunction.

Update on PlayStation Network and Qriocity

Thank you for your patience while we work to resolve the current outage of PlayStation Network & Qriocity services. We are currently working to send a similar message to the one below via email to all of our registered account holders regarding a compromise of personal information as a result of an illegal intrusion on our systems. These malicious actions have also had an impact on your ability to enjoy the services provided by PlayStation Network and Qriocity including online gaming and online access to music, movies, sports and TV shows. We have a clear path to have PlayStation Network and Qriocity systems back online, and expect to

restore some services within a week.

We re working day and night to ensure it is done as quickly as possible. We appreciate your patience and feedback.

Sony Customer Notification US States (excluding Puerto Rico and Massachusetts)

Valued PlayStation Network/Qriocity Customer:

We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network. In response to this intrusion, we have:

Temporarily turned off PlayStation Network and Qriocity services;
Engaged an outside, recognized security firm to conduct a full and complete investigation into what happened; and
Quickly taken steps to enhance security and strengthen our network infrastructure by re-building our system to provide you with greater protection of your personal information.

We greatly appreciate your patience, understanding and goodwill as we do whatever it takes to resolve these issues as quickly and efficiently as practicable.

Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained.

For your security, we encourage you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Sony will not contact you in any way, including by email, asking for your credit card number, social security number or other personally identifiable information. If you are asked for this information, you can be confident Sony is not the entity asking. When the PlayStation Network and Qriocity services are fully restored, we strongly recommend that you log on and change your password. Additionally, if you use your PlayStation Network or Qriocity user name or password for other unrelated services or accounts, we strongly recommend that you change them, as well. To protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. We are providing the following information for those who wish to consider it:

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.
We have also provided names and contact information for the three major

U.S. credit bureaus below. At no charge, U.S. residents can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Experian: 888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013 Equifax: 800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

You may wish to visit the web site of the U.S. Federal Trade Commission at www.consumer.gov/idtheft or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; telephone (877) 566-7226; or www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; telephone: (888) 743-0023; or www.oag.state.md.us.

We thank you for your patience as we complete our investigation of this incident, and we regret any inconvenience. Our teams are working around the clock on this, and services will be restored as soon as possible. Sony takes information protection very seriously and will continue to work to ensure that additional measures are taken to protect personally identifiable information. Providing quality and secure entertainment services to our customers is our utmost priority. Please contact us at 1-800-345-7669 should you have any additional questions.

Sincerely,

Sony Computer Entertainment and Sony Network Entertainment

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Internet Survives Royal Wedding, Scammers Still Lurking

The royal wedding went off without a hitch Friday morning, and the Internet appeared to survive the event as well. Web traffic was high during the nuptials, but YouTube was able to stream the event live to millions around

the world without choking (much). Twitter's fail whale managed to stay off the royal guest list, but online scammers are just getting started with their royal wedding scams and shenanigans. Here's a breakdown of the online highs and lows during Prince William's marriage to Catherine Middleton on Friday.

Global Web usage was big during the royal wedding, but it appears most of the United States decided to stay in bed during the event, or watch in on TV.

The highest Web usage at the time was in the United Kingdom and Western Europe, while United States Web traffic remained normal. That may be the reason why the highly-anticipated event at London's Westminster Abbey didn't appear to be having the same impact online that other major events have had, such as June 24, 2010, the day World Cup qualifying matches and the longest ever Wimbledon match happened at the same time.

News consumption was also high during the ceremony, with a peak of more than 4.5 million page views per minute according to data from Akamai's Net Usage Index. Royal wedding news consumption Friday was higher than when the news of Michael Jackson's death broke in 2009. Akamai reported a high of 4.2 million page views per minute when the King of Pop passed.

Twitter was joking when the company snapped this photo of co-founder Biz Stone dedicating a company server to royal wedding traffic. But Twitter must have done something right, because the company's infamous fail whale was a no-show during the wedding.

And Twitter users were definitely obsessed with the British Monarchy early Friday. Every Twitter trending topic in the USA was wedding-related, as were the network's worldwide topics.

One big discussion was about the similarities between Catherine Middleton's wedding dress and the dress worn by Grace Kelly when the actress married the Prince of Monaco in 1956.

Security firm Sophos uncovered an interesting royal wedding-themed game on social networks that could lead you to revealing important information about yourself. The game asked you to put your "royal wedding guest name" into your status update. You did this by taking the first name of one of your grandparents and then creating a hyphenated last name by merging the name of your first pet with the name of the street you grew up on.

See the problem? Those are all typical answers to security questions used to verify your identity online for Webmail accounts and other services. "The few seconds worth of amusement you may get by telling people your royal wedding guest name are not worth the potential pain of having your identity stolen," Sophos warns.

Now that the nuptials are over, people all over the world will be searching for royal wedding information, including images of Catherine Middleton's dress.

But F-Secure is warning would-be dress hunters to tread carefully online today. Since the dress is likely to be a hot topic of online discussion and Web searches, it's a prime target for black hat search engine optimization pirates trying to lure unsuspecting royal watchers into their traps.

F-Secure already uncovered a scareware attack site when doing a Google Image search for the query "royal wedding coverage." Scareware sites attempt to rip you off by convincing you to buy and install a rogue antivirus program on your computer. Google and Bing do a pretty good job of protecting you from malware, but the best way to keep yourself safe is to only visit sites you trust when looking for royal wedding information.

Google also got into the royal wedding festivities with a Google Doodle on Google UK depicting wedding-themed sites in London.

Recent Incidents Call Web Security Into Question

It s been a busy few weeks in the world of Web security. We saw the computer virus turn 40, a sophisticated cyberattack on a security firm and a major data breach on an email marketer that put millions of customers at risk.

These events have caused considerable chatter among security analysts. Some have pondered whether the security firms we all count on to guard the Internet s infrastructure are capable of protecting themselves. And, if not, what does that mean for everyone s personal security?

The data breach at e-mail marketer Epsilon last month reportedly put millions of users at risk and was possibly the largest breach ever. Customers of big companies such as Citibank, JPMorgan Chase, Target and Walgreens were affected, and now may be at increased risk of e-mail swindles. An increased number of e-mail spam and phishing attacks are expected on victims of the Epsilon breach, according to PC World.

Last month s sophisticated cyberattack on RSA’s SecurID product for two-factor authentication has been referred to as an Advanced Persistent Threat attack. The phrase is often used to describe stealthy and long-term breaches by a foreign country or rival organization designed to obtain valued corporate information such as customer data and intellectual property.

Anup Ghosh, founder and chief scientist of browser security firm Invincea, told PC World that recent events point to a need by security firms to re-evaluate their approach to protecting themselves and their valuable intellectual property.

"We have to worry whether we are going to be targeted next - we, as in the royal we," Ghosh says. "And all we’re really doing is doubling down on the technologies that (were) built in the late ’90s and address yesterday’s problems rather than the way that these attacks are actually perpetrated."

Much has changed since that decade, when only 1,300 viruses were infecting PCs. And it s a completely different technological universe from when the first virus popped up on computer screens in 1971. More than 200 million viruses exist today. Email spam and phishing attacks are on the rise. There s no sign of cybercrime slowing down. At the same time, arming oneself with information, exercising caution and skepticism and taking advantage of PC security products can go a long way in ensuring one s safety on the Internet.

Several analysts expressed concern about the recent security breaches impact on the general public, particularly novice Internet users. Some

worried novice users affected by the Epsilon incident might not go through the trouble of examining the header of each potentially suspicious e-mail. And several sources admitted that details were scarce and specific threats or subsequent precautions couldn t be determined.

In the absence of such information, experts instead reiterated several recommendations for optimizing safety on the Internet. If possible, experts recommend avoiding clicking on links or opening attachments placed in unsolicited emails. The link can take you to a nefarious website, which can infect your computer and the attachment may download software that will track your computer keystrokes, including the passwords you type.

Otherwise, they offer the following tips:

Open a new browser and visit the website that supposedly sent the email; check to see if it’s promoting the same offer that has been sent to you unsolicited.

Mouse over the link contained in the email and look at the lower left corner of the screen to see if the domain name matches the company that is purportedly sending the email.

If you must click on the link, once it’s open it should still show the same domain name. If it doesn’t - and it asks you for financial information like a bank account number or social security number, do not provide the information. If the opened link now has a different domain name, although it’s not requesting financial information, the identity thief may have opted to infect your computer with a virus.

Experts also say keeping security software updated is crucial in arming yourself against cybercrime. Several additional products can also offer a layered approach to Web security. For example, ID Vault complements existing security software by protecting your online transactions. ID Vault prevents users from inadvertently signing in to fraudulent sites or being victimized by phishing, pharming, keystroke logging or other cybercrimes. It helps secure online transactions, locking out hackers and identity thieves, while stopping you from accidentally giving away your personal information.

In addition, LifeLock can add another layer of protection should your information be compromised and misused as the result of a security breach. LifeLock identity theft protection is a proactive defense system that monitors your identity and alerts you whenever it detects your personal information being used. If an application is fraudulent, the remediation team will work to help protect your name.

Finally, experts suggest best Web security practices call for a focus on security for social media applications and the use of those applications and Web sites, strong passwords and PINs and avoiding e-mail or phone-based requests for personal information.

FBI Probes of Some Cyber Attacks Face Troubles

FBI agents have had trouble investigating cyber attacks involving national security because they lack the needed technical expertise or are often transferred or diverted to other cases, according to a government report released on Wednesday.

Sensitive government computer networks are under regular attack from hackers seeking to steal classified material or to cripple critical operations. About 19 percent of the FBI’s cyber agents focus on national security cases.

Some cyber agents complained they did not have the proper experience to investigate such cases, were assigned to other matters or were rotated between offices too often, according to a report by the Justice Department’s inspector general.

"Because national security intrusion cases are highly technical and require a specific set of skills, new cyber agents are often not equipped to assume responsibility of a national security intrusion investigation," the report said.

Further, field agents do not have enough tactical analytical support for those cases, "hampering their ability to connect the dots in an investigation and to determine those responsible for intrusions," it said.

The FBI in 2007 issued a plan for agents to become experts for cyber security investigations with 12 core courses and expected them to complete it along with on-the-job training in five to seven years. The number of agents who have completed the coursework was not made public in the report.

The inspector general’s office tested 36 cyber agents it interviewed to see if they had the technical skills for national security cases and found that 64 percent did.

Five of the 36 field agents interviewed said that they did not think they were able to effectively investigate national security intrusions and were not qualified to do so, according to the inspector general’s report.

The FBI told the inspector general that it was looking into the concerns about transfers and that the cyber division has also begun realigning its career path program to ensure "field offices had qualified agents to investigate national security intrusion matters," the report said.

The inspector general also recommended that the FBI create regional hubs with cyber agents who can deal with the national security cases, an idea the agency said it was considering.

NY Case Underscores Wi-Fi Privacy Dangers

Lying on his family room floor with assault weapons trained on him, shouts of "pedophile!" and "pornographer!" stinging like his fresh cuts and bruises, the Buffalo homeowner didn’t need long to figure out the reason for the early morning wake-up call from a swarm of federal agents.

That new wireless router. He’d gotten fed up trying to set a password. Someone must have used his Internet connection, he thought.

"We know who you are! You downloaded thousands of images at 11:30 last night," the man’s lawyer, Barry Covert, recounted the agents saying. They referred to a screen name, "Doldrum."

"No, I didn’t," he insisted. "Somebody else could have but I didn’t do anything like that."

"You’re a creep ... just admit it," they said.

Law enforcement officials say the case is a cautionary tale. Their advice: Password-protect your wireless router.

Plenty of others would agree. The Sarasota, Fla. man, for example, who got a similar visit from the FBI last year after someone on a boat docked in a marina outside his building used a potato chip can as an antenna to boost his wireless signal and download an astounding 10 million images of child porn, or the North Syracuse, N.Y., man who in December 2009 opened his door to police who’d been following an electronic trail of illegal videos and images. The man’s neighbor pleaded guilty April 12.

For two hours that March morning in Buffalo, agents tapped away at the homeowner’s desktop computer, eventually taking it with them, along with his and his wife’s iPads and iPhones.

Within three days, investigators determined the homeowner had been telling the truth: If someone was downloading child pornography through his wireless signal, it wasn’t him. About a week later, agents arrested a 25-year-old neighbor and charged him with distribution of child pornography. The case is pending in federal court.

It’s unknown how often unsecured routers have brought legal trouble for subscribers. Besides the criminal investigations, the Internet is full of anecdotal accounts of people who’ve had to fight accusations of illegally downloading music or movies.

Whether you’re guilty or not, "you look like the suspect," said Orin Kerr, a professor at George Washington University Law School, who said that’s just one of many reasons to secure home routers.

Experts say the more savvy hackers can go beyond just connecting to the Internet on the host’s dime and monitor Internet activity and steal passwords or other sensitive information.

A study released in February provides a sense of how often computer users rely on the generosity - or technological shortcomings - of their neighbors to gain Internet access.

The poll conducted for the Wi-Fi Alliance, the industry group that promotes wireless technology standards, found that among 1,054 Americans age 18 and older, 32 percent acknowledged trying to access a Wi-Fi network that wasn’t theirs. An estimated 201 million households worldwide use Wi-Fi networks, according to the alliance.

The same study, conducted by Wakefield Research, found that 40 percent said they would be more likely to trust someone with their house key than with their Wi-Fi network password.

For some, though, leaving their wireless router open to outside use is a philosophical decision, a way of returning the favor for the times they’ve hopped on to someone else’s network to check e-mail or download directions while away from home .

"I think it’s convenient and polite to have an open Wi-Fi network," said Rebecca Jeschke, whose home signal is accessible to anyone within range.

"Public Wi-Fi is for the common good and I’m happy to participate in that - and lots of people are," said Jeschke, a spokeswoman for the Electronic Frontier Foundation, a San Francisco-based nonprofit that takes on cyberspace civil liberties issues.

Experts say wireless routers come with encryption software, but setting it up means a trip to the manual.

The government’s Computer Emergency Readiness Team recommends home users make their networks invisible to others by disabling the identifier broadcasting function that allows wireless access points to announce their presence. It also advises users to replace any default network names or passwords, since those are widely known, and to keep an eye on the manufacturer’s website for security patches or updates.

People who keep an open wireless router won’t necessarily know when someone else is piggybacking on the signal, which usually reaches 300-400 feet, though a slower connection may be a clue.

For the Buffalo homeowner, who didn’t want to be identified, the tip-off wasn’t nearly as subtle.

It was 6:20 a.m. March 7 when he and his wife were awakened by the sound of someone breaking down their rear door. He threw a robe on and walked to the top of the stairs, looking down to see seven armed people with jackets bearing the initials I-C-E, which he didn’t immediately know stood for Immigration and Customs Enforcement.

"They are screaming at him, ’Get down! Get down on the ground!’ He’s saying, ’Who are you? Who are you?’" Covert said.

"One of the agents runs up and basically throws him down the stairs, and he’s got the cuts and bruises to show for it," said Covert, who said the homeowner plans no lawsuit. When he was allowed to get up, agents escorted him and watched as he used the bathroom and dressed.

The homeowner later got an apology from U.S. Attorney William Hochul and Immigration and Customs Enforcement Special Agent in Charge Lev Kubiak.

But this wasn’t a case of officers rushing into the wrong house. Court filings show exactly what led them there and why.

On Feb. 11, an investigator with the Department of Homeland Security, which oversees cybersecurity enforcement, signed in to a peer-to-peer file sharing program from his office. After connecting with someone by the name of "Doldrum," the agent browsed through his shared files for videos and images and found images and videos depicting children engaged in sexual acts.

The agent identified the IP address, or unique identification number, of the router, then got the service provider to identify the subscriber.

Investigators could have taken an extra step before going inside the house and used a laptop or other device outside the home to see whether there was an unsecured signal. That alone wouldn’t have exonerated the homeowner, but it would have raised the possibility that someone else was responsible for the downloads.

After a search of his devices proved the homeowner’s innocence, investigators went back to the peer-to-peer software and looked at logs that showed what other IP addresses Doldrum had connected from. Two were associated with the State University of New York at Buffalo and accessed using a secure token that UB said was assigned to a student living in an apartment adjacent to the homeowner. Agents arrested John Luchetti March 17. He has pleaded not guilty to distribution of child pornography.

Luchetti is not charged with using his neighbor’s Wi-Fi without permission. Whether it was illegal is up for debate.

"The question," said Kerr, "is whether it’s unauthorized access and so you have to say, ’Is an open wireless point implicitly authorizing users or not?’

"We don’t know," Kerr said. "The law prohibits unauthorized access and it’s just not clear what’s authorized with an open unsecured wireless."

In Germany, the country’s top criminal court ruled last year that Internet users must secure their wireless connections to prevent others from illegally downloading data. The court said Internet users could be fined up to $126 if a third party takes advantage of their unprotected line, though it stopped short of holding the users responsible for illegal content downloaded by the third party.

The ruling came after a musician sued an Internet user whose wireless connection was used to download a song, which was then offered on an online file sharing network. The user was on vacation when the song was downloaded.

ICANN Names Computer Hacker as Security Chief

Jeff Moss, a prominent computer hacker who founded the annual Black Hat and DefCon security conferences in Las Vegas, has been hired as the chief security officer for the organization that coordinates names of the world’s Web sites.

The organization, the Internet Corporation for Assigned Names and Numbers, or ICANN, plays a vital role in making sure that when you type a site name into a Web browser, your computer knows where to go to find the site you’re trying to reach. ICANN manages the domain name system that underlies that chain of communication.

"I can think of no one with a greater understanding of the security threats facing Internet users and how best to defend against them than Jeff Moss," Rod Beckstrom, ICANN’s CEO and formerly the director of the U.S. National Cybersecurity Center, said in a statement. "He has the in-depth insider’s knowledge that can only come from fighting in the trenches of the ongoing war against cyber threats."

Moss, who also serves on the U.S. Department of Homeland Security’s advisory council, takes on the new post Friday at ICANN’s offices in Washington, D.C.

Amazon Apologizes for EC2 Cloud Outage

Now that the dust has settled on the Amazon EC2 cloud outage, the company is offering an apology and a credit for its role in making many popular web sites, like FourSquare, Twitter, and Netflix, unavailable.

Amazon Elastic Book Store customers in regions affected at the time of the disruption, regardless of whether their resources and application were impacted or not, are getting an automatic 10-day credit equal to 100 percent of their usage.

"We know how critical our services are to our customers' businesses and we will do everything we can to learn from this event and use it to drive improvement across our services," Amazon said in a statement. "As with any significant operational issue, we will spend many hours over the coming days and weeks improving our understanding of the details of the various parts of this event and determining how to make changes to improve our services and processes."

Most anyone familiar with data center operations could sympathize with Amazon - outages, even severe outages, happen, and companies are usually judged according to how quickly they respond to the problem and whether they are able to prevent similar events from occurring again, said Charles King, principal analyst at Pund IT.

However, he added, while Amazon's cloud services are generally well regarded, patience among affected companies and their clients wore thin as the days stretched on. That was hardly surprising, he said, but it created the opportunity to consider exactly how organizations have been leveraging the EC2 cloud, and how well they've been doing it.

"Some, including Netflix and SmugMug, were hardly affected at all, largely because they had designed their environments for high availability - in line with Amazon's guidelines - using EC2 as merely one of several IT resources," King said. "On the other hand, those that had depended largely or entirely on Amazon for their online presence came away badly burned."

King sees two key, albeit it not exactly new, lessons in the Amazon cloud outage. First, systems that rely on single points of failure will fail at some point. Second, companies whose services depend largely or entirely on third parties can do little but complain, apologize, pray and twiddle their thumbs when things go south.

As King sees it, the fact that disaster is inevitable is why good communications skills are so crucial for any company to develop, and why Amazon's anemic public response to the outage made a bad situation far worse than it needed to be. While the company has been among the industry's most vocal cloud services cheerleaders, King said, it seemed essentially tone deaf to the damage its inaction was doing to public perception of cloud computing.

"At the end of the day, we expect Amazon will use the lessons learned from the EC2 outage to significantly improve its service offerings," King said. "But if it fails to closely evaluate communications efforts around the event, the company's and its customers' suffering will be wasted."

Go and Sin No More: DOJ Oversight of Microsoft Ending

Microsoft won’t be under a microscope any more come May - at least not from the Department of Justice. The software giant has been dealing with regulators for 13 years, after the DOJ filed an antitrust lawsuit.

The DOJ accused Microsoft of using its market heft to roll over competitors. Words like monopoly were used. But judges in the case seem ready to allow that oversight to end, and the DOJ will stop scrutinizing Microsoft’s moves as of May 12.

"And so May 12 will close an important chapter in the history of antitrust law," said Judge Colleen Kollar-Kotelly during the last oversight hearing on Wednesday at the U.S. District Court for the District of Columbia, according to Reuters.

The DOJ and attorneys general for 19 states plus the District of Columbia filed suit against Microsoft in 1998 claiming violations of antitrust laws.

After discussions ordered by the federal court, Microsoft reached a settlement - often referred to as the consent decree - with the DOJ in 2001. Nine states joined in that agreement while seven others continued to pursue their claims separately before accepting the District Court’s final judgment in 2002. One state appealed the ruling, but it was upheld in 2004 by the U.S. Court of Appeals.

Following the antitrust action, Microsoft faced a number of class-action lawsuits. But unlike the government case, which alleged that Microsoft used its market position to harm competition by incorporating new features into the Windows operating systems at no additional cost, the private class-action suits claimed Microsoft overcharged consumers.

It was a nightmare for Microsoft that few in the technology industry will soon forget. But now that it appears to be over, or at least almost over, the market may see a bolder Microsoft. Indeed, the expiration of DOJ oversight will allow the software giant more freedom to compete, according to Rob Enderle, principal analyst at the Enderle Group.

"Any type of consent decree like the one that was over IBM and the one that is over Microsoft limits significantly a company’s ability to move," Enderle said. "They have to always be worried that something they are doing or considering or strategizing is going to cross the line or get them in trouble by the folks providing the oversight. The fear of that can tie a company up badly."

As Enderle sees it, Microsoft could not enter into certain discussions or follow certain paths for fear it might offend the DOJ. Just the fear that the DOJ is looking over your shoulder makes it easy to consider almost any move controversial, he said.

"If a manager doesn’t like an idea because it wasn’t their idea, they can raise this specter of regulatory oversight and be very effective at killing it," Enderle said. "That just ties the company up. It changes the company from a firm that’s run by product managers to a firm that’s run by attorneys. Not only is that not a great place to work, it also makes a firm overly rigid. It doesn’t allow it to bring its A game."

Sony Shows Tablets To Compete with Apple Offerings

Sony is planning a tablet computer with a touch panel similar to Apple’s iPad for later this year that the Japanese manufacturer promises will make the best of its gadgetry and entertainment strengths.

The product code-named S1, shown Tuesday in Tokyo, comes with a 9.4 inch display for enjoying online content, such as movies, music, video games and electronics books, and for online connections, including email and social networking.

Sony, which boasts electronics as well as entertainment divisions, also showed S2, a smaller mobile device with two 5.5 inch displays that can be folded like a book.

It did not give prices. Sony Corp. Senior Vice President Kunimasa Suzuki said the products will go on sale worldwide from about September. Both run Google’s Android 3.0 operating system.

The announcement of Sony’s key net-linking offerings comes as it tries to fix the outage of its PlayStation Network, which offers games and music online.

It is unclear when that can start running again. Sony has blamed the problem on an "external intrusion" and has acknowledged it would have to rebuild its system to add security measures and strengthen its infrastructure.

Suzuki said both of the latest tablets feature Sony’s "saku saku," or nifty, technology that allows for smooth and quick access to online content and for getting browsers working almost instantly after a touch.

"We offer what is uniquely Sony," Suzuki said after demonstrating how the S1 was designed with a tapered width for carrying around "like a magazine."

The devices will connect to Sony’s cloud-computing based library of content such as movies and music, as well as to Sony PlayStation video games adapted for running on Android and digital books from Sony’s Reader store, the company said.

Sony, which makes the Vaio personal computer and PlayStation 3 video game console, has lost some of its past glory - once symbolized in its Walkman portable music player that pioneered personal music on-the-go in the 1980s, catapulting the Japanese company into a household name around the world.

It has been struggling against flashier and more efficient rivals including Apple Inc. of the U.S. with its iPhone, iPod and iPad machines, as well as South Korea’s Samsung Electronics Co., from which Sony purchases liquid-crystal displays, a key component in flat-panel TVs.

Sony has already promised a successor to its PlayStation Portable machine for late this year, code-named NGP for "next generation portable," promising the quality of a home console in an on-the-go machine boasting a screen double the size of smart phones.

The popularity of smart phones including the iPhone has been another threat to Sony.

Kazuo Hirai, promoted in March to head Sony’s sprawling consumer products and services division, said Sony’s strategy has always been about combining the benefits of hardware, software and networking to make consumers happy, and that was the same goal for S1 and S2.

"There is no change to that approach," he said.

10 Must-Have Free Firefox 4 Add-Ons

The recently released Firefox 4 is a big improvement over previous versions of the popular Web browser, but you can still teach it plenty of tricks.

We’ve rounded up ten great downloads to help you get more out of Firefox 4. Not all older add-ons work with Firefox 4, but every one in this roundup does. Whether you want to enhance search, better manage the information you find online, keep yourself safe, or perform other Web tasks, we have what you need. And all of these picks are free.

Power Up Search

A good part of your browsing day consists of a single task: searching the Web. These three add-ons can help make searching in Firefox better, easier, and more productive.

Apture Highlights. With this add-on, you can highlight a word or phrase and then click a ’Learn More’ bubble to get information from Wikipedia, links to YouTube, search results on Google and Bing, and photos related to the words. If you’ve highlighted a location, you can see a map in Google Maps.

InstantFox solves the problem, allowing you to use Firefox’s address bar to perform searches. For example, to search Google for Android, type *g Android* into the address bar. You can add other letters before a search term to search other sites, such as *a* for Amazon, *yh* for Yahoo, and *y* for YouTube.

KwiClick lets you highlight a word or phrase to obtain more information. In this case highlighting produces a cloverleaf icon with four leaves - one for each search and information provider, set by default as Google, Wikipedia, YouTube, and Google Maps. Click any icon, and you’ll see information from that site in another window. You can customize the icon with many other providers, as well.

Because Apture Highlights and KwiClick work the same way, they conflict with each other when both are installed. If you’d like to keep both, however, you can use a workaround. Apture Highlights takes precedence over KwiClick; when you highlight a word or phrase and hover your mouse over it, the Apture Highlights ’Learn More’ bubble appears, while the KwiClick cloverleaf remains hidden and inaccessible in the background. But if you highlight a word or phrase and then right-click, you’ll see a KwiClick option on the menu. Choose that item to bring up the KwiClick window.

Manage Online Information

Suffering from information overload? Who isn't? The following two Firefox add-ons make gathering information--and keeping it organized once you've found it - easier.

Feedly, you can create your own personalized online newspaper by gathering stories and blog posts from news sources across the Web. It constantly self-updates, so whenever you check it, the latest news is always available. Feedly uses RSS technology and starts off with a prebuilt set of feeds, but you can easily customize them. It also integrates with Google Reader, so if you've already built up feeds there, it'll grab those for you as well.

Read It Later is for you. When you're on a page that you want to save, click the small icon to the right of the Firefox address bar. You can then go back and read the item whenever you want, via the Firefox add-on, from the Web itself, or on another computer or mobile device with a Read It Later add-on.

To read saved articles and pages, you click a Read It Later icon that's separate from the one you use to save the pages. There's a chance that the icon won't initially appear, however. To make it show up in Firefox 4, click the orange Firefox button at the upper-left corner of the screen, select /Options, Toolbar layout,/ and then drag the Read It Later icon to the Firefox toolbar.

Protect Yourself Online

The Web can be dangerous, with malicious software and hackers targeting you and trying to steal your private information. But you can combat such threats with these two Firefox add-ons.

NoScript, you can block them from running, permit them to run just once, or allow them to run every time you visit sites that you know and trust.

BetterPrivacy hunts them down and zaps them to erase your trail.

Miscellaneous Add-Ons

Check out these three handy tools to find out about the weather, block ads, and more effectively manage multiple Web pages.

ForecastFox Weather delivers weather reports straight to Firefox. After you install it and choose your area of interest, the appropriate weather information appears at the bottom right of your browser. Just hover your mouse over the display to see even more details.

Adblock Plus. It gives you control over what to block and what to let through, so you can block ads on some sites and enable them on others. You can also fine-tune the add-on so that it only blocks ads and doesn't interfere with site functionality.

FoxTab, you can control browser tabs through a 3D interface. In addition to being pretty, the interface gives you greater control and includes a Safari-like feature that shows your favorite sites every time you open a new tab.

Happy 30th Birthday, Computer Mouse!

Thirty years ago today, the first computer mouse to be used alongside a personal computer appeared. On April 27, 1981, the integrated mouse made its debut with the Xerox Star Information System.

First called "Computer-Aided Display Control," the term "mouse" referred to the tool’s rounded shape and wire "tail" protruding out the back of the gadget that gave it a rodent-like look.

The mouse has come a long way in its 30 years. Most don’t even have wires any more, especially in an era where so many tech companies are producing touch-screen technology with devices like Apple’s iPhone or other smartphones and tablets. Additionally, most laptops use some sort of touchpad to navigate the screen, or a pointer stick.

The prototype for the first mouse was invented by Douglas Englebard in 1963 while he was working at Palo Alto’s Stanford Research Institute. Before it morphed into the mouse that is commonly seen today, it went through many different forms. For example, one method was mounting a device on the user’s head or chin. In 1972, wheels on the bottom of the mouse were replaced by a trackball, a feature that many mice don’t even use today.

The device went through many revisions before Xerox released it with star in 1982. However, the mouse didn’t get a lot of attention until it appeared with Apple’s Macintosh three years later.

Can you imagine the computer without the mouse? PCMag’s John Dvorak gives the mouse a lot of credit for the rise of the Internet.

Computer mice have been an integral part of the tech age, and evolved quite a bit in the three decades since their debut.

Guillen Suspended for Twitter Blast

Major League Baseball slapped Ozzie Guillen with a two-game ban after the Chicago White Sox manager used Twitter to complain about begin ejected from a game.

Guillen, who was also fined, was tossed out of Wednesday’s White Sox game for arguing balls and strikes. MLB declined to release the amount of the fine.

It marks the first time American baseball has suspended a manager or player for using Twitter during a game.

Guillen, who was ejected by plate umpire Todd Tichenor during a game against the New York Yankees, wrote on his Twitter page that the ejection was "pathetic".

Guillen will miss two games against the Baltimore Orioles.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.